

**BEFORE THE ODISHA ELECTRICITY REGULATORY COMMISSION,  
BIDYUT NIYAMAK BHAWAN.  
PLOT No-4, CHUNOKOLI, SHAILASHREE VIHAR, BHUBANESWAR-751021**

Case No: \_\_\_\_ of 2026

**IN THE MATTER OF:** Application under Para 3.2 of the OERC (Terms and Conditions for determination of Wheeling Tariff and Retail Supply Tariff) Regulations, 2022 for approval of Supplementary Capital Investment Plan for FY 2026-27 for implementation of Cybersecurity Solutions in the Licensed area of TP Central Odisha Distribution Ltd.

**AND**

**IN THE MATTER OF:** TP Central Odisha Distribution Ltd., Corporate Office, Power House, Unit 8, Bhubaneswar- 751 012 represented by its Chief-Regulatory & Legal.

...Petitioner

**IN THE MATTER OF:**

M/s GRIDCO, M/s. OPTCL, M/s. SLDC, Department of Energy, Govt. of Odisha and All Concerned Stake Holders

...Respondent

Affidavit

10 JUN 2026

I, Bharat Kumar Bhadawat, aged about 54 Years, son of late Shri Shankar Lal Bhadawat residing at Bhubaneswar do hereby solemnly affirm and say as follows:

1. I am the Chief-Regulatory & Legal of TP Central Odisha Distribution Ltd. the petitioner in the above matter and I am duly authorized to swear this affidavit on its behalf.

The statements made in the submission herein shown to me are based on information provided to me and I believe it to be true.

Bhubaneswar.

Dated: 10<sup>th</sup> June 2026

  
Bharat Kumar Bhadawat

Chief- Regulatory & Legal

  
Identified by  
Advocate

No Dependent address named being identified by   
Advocate at appears before me on 10/06/2026 at about 3:35 A.M.  
P.M. and states on oath that the contents of this affidavit are true to the best of his/her knowledge.

  
ANIL KUMAR MOHANTY  
NOTARY, BBSR  
REED. No. - @N-116/2000

**BEFORE THE ODISHA ELECTRICITY REGULATORY COMMISSION,  
BIDYUT NIYAMAK BHAWAN.  
PLOT No-4, CHUNOKOLI, SHAILASHREE VIHAR, BHUBANESWAR-751021**

Case No. \_\_\_\_ of 2026

**IN THE MATTER OF:** Application under Para 3.2 of the OERC (Terms and Conditions for determination of Wheeling Tariff and Retail Supply Tariff) Regulations, 2022 for approval of Supplementary Capital Investment Plan for FY 2026-27 for implementation of Cybersecurity Solutions in the Licensed area of TP Central Odisha Distribution Ltd.

**IN THE MATTER OF:** TP Central Odisha Distribution Ltd., Corporate Office, Power House, Unit 8, Bhubaneswar- 751 012 represented by its Chief-Regulatory & Legal.

.... *Petitioner*

**IN THE MATTER OF:** M/s. GRIDCO, M/s. OPTCL, M/s. SLDC, Department of Energy, Govt. of Odisha and All Concerned Stake Holders.

.... *Respondents*

**Most Respectfully Sheweth,**

1. That, the Petitioner DISCOM, has taken over the distribution business from erstwhile CESU utility w.e.f 01.06.2020 as per terms of vesting order. TP Central Odisha Distribution Limited (TPCODL) is a joint venture between The Tata Power Company Ltd. and the Government of Odisha with equity participation in the ratio of 51% : 49% respectively.
2. That, the Petitioner is the Distribution Licensee, as per License Condition dated 24.08.2020 of the Hon'ble Commission, in central part of Odisha having five Distribution Circle namely Bhubaneswar-I, Bhubaneswar-II, Cuttack, Dhenkanal and Paradeep with area of operation of 29354 Sq.Km.
3. That, the Petitioner DISCOM is required to "supply electricity" in accordance with the provisions as laid down under section 42 of the Electricity Act, 2003.
4. That, as per mandate of Vesting Order, the Petitioner is procuring power from GRIDCO, who is the state designated entity to procure power for all the 4 DISCOM(s) from different generators like Thermal, Hydel, Renewable etc. located in and outside Odisha.

**A. Background for Submission of the Petition**



*Beswada*

5. In compliance with the directives stipulated in the Vesting Order dated 26.05.2020 as well as the Odisha Electricity Regulatory Commission (Terms and Conditions for Determination of Wheeling Tariff and Retail Supply Tariff) Regulations 2014 and 2022, TPCODL since its commencement of operation has been submitting its Capital Investment plan every year for the approval of the Hon'ble Commission.
6. The Odisha Electricity Regulatory Commission (Terms and Conditions for Determination of Wheeling Tariff and Retail Supply Tariff) Regulations, 2022 (hereinafter referred to as "Tariff Regulations, 2022") requires submission of a Capital Investment Plan for each year of the Control Period. The relevant regulatory framework provides as follows:

*"3.2.1. The Distribution Licensee shall submit detailed capital investment plan, financing plan and physical targets for each year of the Control Period for strengthening and augmentation of distribution network, meeting the requirement of load growth, reduction in distribution losses, improvement in quality of supply, reliability, metering, reduction in congestion, etc., to the Commission for approval, as a part of the Business Plan applicable for the entire control period and annual proposal for each year of the Control Period.*

*"3.2.2. The Distribution Licensee shall file a separate annual Capital Investment Plan comprising of capital investment plan, financing plan and physical targets for each year of the Control Period as per the timelines specified in Annexure-I."*

7. In compliance to the above provision of the Tariff Regulations, 2022 the petitioner has submitted its Capital Investment Plan for FY 2026-27 vide submission dated 10.09.2025 (registered as Case No-77 /2025).
8. The Hon'ble Commission in its order dated 15.05.2026 in the above case matter (i.e. Case No. 77 /2025) has approved total Capex of Rs. 485.67 Cr against Rs. 570 Cr proposed by the petitioner. We are thankful to the Hon'ble Commission for approving the capex for FY 2026-27.
9. Subsequent to the submission of above application, various cyber security related incidents have been witnessed in various Organizations across the Globe including some of the Tata Group companies (some of the examples are provided in table below). The impact of these incidents are serious including huge financial losses and prolonged disruption of business operations. Power Distribution being a critical infrastructure, this emerging threat has become a serious cause of concern for the petitioner.



| S. No | Organization Name | Description                                                                               | Month of Incident | Root Cause                                                                              | Impact                                                                                                                                                                 | Learning                                                              |
|-------|-------------------|-------------------------------------------------------------------------------------------|-------------------|-----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| 1     | Jaguar Land Rover | Attack carried out by Group-Scattered Lapsus Hunters forced shutdown of production line.  | Aug/<br>Sep'25    | Lack of Real Time Visibility into Cyber-attack.<br>Limited Incident Response Capability | Over 2 Billion Pounds in Direct Losses<br>All major global facilities halted.<br>Loss of customer and employee Trust<br>Impacting an estimated 104,000 jobs in the UK. | Deployment of SIEM/SOAR/UEBA Tools for 24X7 and Proactive monitoring. |
| 2     | Tata Digital      | Tata 1MG experienced a major ransomware attack on its IT Systems.                         | May'25            | Lack of Real Time Visibility into Cyber-attack.<br>Limited Incident Response Capability | Operations Impact.<br>Sensitive Data Theft<br>Loss of customer Trust                                                                                                   | Deployment of SIEM/SOAR/UEBA Tools for 24X7 and Proactive monitoring. |
| 3     | Tata Technologies | Tata Technologies experienced a ransomware attack by Hunters by exploiting Database level | Jan'25            | Lack of Real Time Visibility into Cyber-attack.<br>Limited Incident Response Capability | Theft of 1.4 TB of confidential company data.<br>Loss of customer Trust<br>Halting of Operations                                                                       | Deployment of SIEM/SOAR/UEBA Tools for 24X7 and Proactive monitoring. |

10. In view of the above, to address this urgent business threat this Capital Investment plan is submitted for enhancing the organization's cyber resilience, protecting critical digital assets, and ensuring compliance with evolving regulatory and operational standards.
11. This requirement was not part of the original capital investment plan for FY 2026-27 submitted in Sep 2025, however because of the subsequent development as explained above, this Supplementary Capital Investment plan is being submitted to address the critical issue of Cyber Security.
12. In this application, we are seeking the approval of the Hon'ble Commission for the proposed Supplementary Capital Investment Plan for FY 2026-27 amounting to Rs. 6.24 Cr (Hard Cost) under the major head of "Technology and Infrastructure" towards deployment of advanced Cybersecurity solutions, namely Security Information and Event Management (SIEM), Security Orchestration Automation & Response (SOAR), End User Behavioral Analysis (UEBA) and other Cybersecurity solutions in compliance with mandatory statutory and regulatory norms as provided in details in the DPR enclosed as **Appendix**.
13. The Board of Directors of TPCODL, at its meeting held on 22nd April 2026, has accorded approval of Rs. 6.24 Cr towards above proposed Capital Investment for FY 2026-27. A certified true copy of the Board Approval is enclosed as **Annexure-I** of the Appendix to this submission

## B. Summary of Submission

14. It is submitted that the need for this supplementary capital investment plans is arising from unforeseen developments and mandatory compliance requirements. The petitioner therefore respectfully submits that the supplementary filing is justified on merits and in the interest of ensuring the security and reliability of the licensed distribution network and the protection of consumer interests.
15. As on date, the petitioner has deployed various Cybersecurity tools like Firewall, Antivirus, Extended Detection and Response (XDR), Web application Firewall, Privilege Access Management, Distributed Denial of Service (DDoS) appliance, etc. to ensure basic Cyber Hygiene. However, the organization lacks real time visibility into any Cyber Attack or breach



*Bea Weidawaf*

scenario. This limitation restricts organization's ability to proactively identify any Cyber-attack and carry out an effective Incident response measure.

16. While the details of the proposal is provided in the **Appendix** which includes scope and objective, purpose of investment, broad technical specifications, cost estimates, cost benefit analysis and physical targets, the summary is provided in table below.

**Table A: Component-wise Break-up of Supplementary Capex (Hard Cost Only)**

| Sl. No. | Component                                         | Amount (Rs. Cr.) |
|---------|---------------------------------------------------|------------------|
| 1       | On-premises Hardware with 5-Year Warranty Support | 0.50             |
| 2       | SIEM / SOAR / UEBA Software Licenses              | 5.52             |
| 3       | Implementation with existing SIEM                 | 0.22             |
|         | <b>Total</b>                                      | <b>6.24</b>      |

17. The above Capital Investment Plan of Rs. 6.24 Cr. as depicted in the table above is hard cost only. The cost towards Employees working on such projects would be in addition to the amount that would be approved by the Hon'ble Commission under this petition.
18. Similarly, the Interest During Construction (IDC) is required to be worked out on the Debt Component (70%) of the Capex. The same would depend on the quantum of the capital expenditure spread during the year. It is submitted that Interest During Construction amount would need to be added in addition to Hard Cost and Employee Cost to be capitalized.

*B. S. Choudhary*



### C. Prayers

TPCODL Prays that the Hon'ble Commission may kindly be pleased to:

1. Approve the Supplementary Capital Investment Plan of Rs. 6.24 Crores (Hard Cost ) for FY 2026-27 which is required for implementation Cybersecurity Solutions in the licensed area of TP Central Odisha Distribution Ltd.
2. Allow Employee Cost and Interest During Construction (IDC), based on actuals, to be capitalized over and above the approved Capex (Hard Cost) for the aforesaid period.
3. Permit carrying forward of any unspent Capital Expenditure under this Capex Plan to subsequent financial year.
4. To kindly condone any inadvertent omission /errors/shortcoming and allow to make future submission as may be required in future to support this application in terms of modification /clarifications, if any.
5. That, the petitioner craves leave for submission of further /additional reply as and when required by the Hon'ble Commission.
6. Any other direction as the Hon'ble Commission may think appropriate.

Bhubaneswar  
Dated:10<sup>th</sup> June 2026

  
**Bharat Kumar Bhadawat**  
Chief – Regulatory & Legal



## **Supplementary Capex Plan for Cybersecurity under Technology & Infrastructure Budget Head for FY26-27**

### **Contents**

|                                                                        |          |
|------------------------------------------------------------------------|----------|
| <b>1. Scope and Objective.....</b>                                     | <b>2</b> |
| <b>2. Purpose of investment.....</b>                                   | <b>2</b> |
| <b>3. Broad Technical Specifications for Proposed Investment .....</b> | <b>4</b> |
| <b>4. Capital Structure .....</b>                                      | <b>4</b> |
| <b>5. Capitalization Schedule.....</b>                                 | <b>5</b> |
| <b>6. Financing Plan .....</b>                                         | <b>5</b> |
| <b>6.1. CAPEX Plan.....</b>                                            | <b>5</b> |
| <b>7. Physical Target/ Activity .....</b>                              | <b>5</b> |
| <b>8. Cost Benefit Analysis.....</b>                                   | <b>5</b> |
| <b>8.1. Tangible (Quantifiable) Benefits.....</b>                      | <b>6</b> |
| <b>8.2. Intangible (Non-Quantifiable) Benefits .....</b>               | <b>6</b> |
| <b>8.3. Summary of Financial Justification .....</b>                   | <b>6</b> |
| <b>9. Approval from Board of Directors (BOD) .....</b>                 | <b>7</b> |

## 1. Scope and Objective

TP Central Odisha Distribution Ltd. (TPCODL) has been successfully serving reliable power supply and providing enhanced customer services to its consumer base. These goals are being achieved through strategic upgrades to existing distribution infrastructure via adoption of advanced IT & OT technologies thereby enabling provision of digital services to customers while ensuring both efficiency and convenience. Although, implementation of advance IT & OT solutions has brought numerous benefits to the consumers and services catered, it has also brought a unique challenge in the form of Cybersecurity.

As on date, TPCODL has deployed various Cybersecurity tools like Firewall, Antivirus, Extended Detection and Response (XDR), Web application Firewall, Privilege Access Management, Distributed Denial of Service (DDoS) appliance, etc. to ensure basic Cyber Hygiene.

However, the organization lacks real time visibility into any Cyber Attack or breach scenario. This limitation restricts organization's ability to proactively identify any Cyber-attack and carry out an effective Incident response measure.

Hence, to ensure the organization have the ability to respond to such critical scenarios, the Discom aspire to deploy Security Information and Event Management (SIEM), Security Orchestration Automation & Response (SOAR) and End User Behavioural Analysis (UEBA) solutions respectively.

This proposal seeks approval for additional CAPEX allocation, under the Budget Head "Technology and Infrastructure" towards the procurement and deployment of advanced cybersecurity solutions.

## 2. Purpose of investment

The primary purpose of this investment is to strengthen cybersecurity posture with addition of real time visibility and analysis of security alerts generated through multiple IT / OT. Considering existing environment and multiple cybersecurity attacks globally, it is pertinent to implement this kind of system which have capability to prevent such incidents and take appropriate actions proactively if situation warrant so.

In the recent global scenarios due to international Geo-political conflicts wherein hacking groups and rogue state sponsored hacking activities have increased substantially leading to major cyber-attacks.

Mentioned below is the list of key Global Cyber security incidents impacting Critical Information Infrastructure:

| S. No | Organization Name | Description                                                                                              | Date        | Root Cause                                                                                                                                       | Impact                                                                                                                                                                                                                                     | Learning                                                              |
|-------|-------------------|----------------------------------------------------------------------------------------------------------|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| 1.    | Jaguar Land Rover | Attack carried out by Group-Scattered Lapsus Hunters forced shutdown of production line.                 | Aug/ Sep'25 | <ul style="list-style-type: none"> <li>Lack of Real Time Visibility into Cyber-attack.</li> <li>Limited Incident Response Capability.</li> </ul> | <ul style="list-style-type: none"> <li>Over 2 Billion Pounds in Direct Losses</li> <li>All major global facilities halted.</li> <li>Loss of customer and employee Trust</li> <li>Impacting an estimated 104,000 jobs in the UK.</li> </ul> | Deployment of SIEM/SOAR/UEBA Tools for 24X7 and Proactive monitoring. |
| 2.    | Tata Digital      | Tata 1MG experienced a major ransomware attack on its IT Systems.                                        | May'25      | <ul style="list-style-type: none"> <li>Lack of Real Time Visibility into Cyber-attack.</li> <li>Limited Incident Response Capability</li> </ul>  | <ul style="list-style-type: none"> <li>Operations Impact.</li> <li>Sensitive Data Theft</li> <li>Loss of customer Trust</li> </ul>                                                                                                         | Deployment of SIEM/SOAR/UEBA Tools for 24X7 and Proactive monitoring. |
| 3.    | Tata Technologies | Tata Technologies experienced a ransomware attack by Hunters by exploiting Database level vulnerability. | Jan'25      | <ul style="list-style-type: none"> <li>Lack of Real Time Visibility into Cyber-attack.</li> <li>Limited Incident Response Capability</li> </ul>  | <ul style="list-style-type: none"> <li>Theft of 1.4 TB of confidential company data.</li> <li>Loss of customer Trust</li> <li>Halting of Operations</li> </ul>                                                                             | Deployment of SIEM/SOAR/UEBA Tools for 24X7 and Proactive monitoring. |

This shall also help organization to comply with various statutory and regulatory notifications as referenced below: -

- Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018 - (j) establish a Cyber Security Operation Centre (C-SOC)** using tools and technologies to implement preventive, detective and corrective controls to secure against advanced and

emerging cyber threats. In addition, Cyber Security Operation Center is to be utilized for identifying unauthorized access to "Protected System", and unusual and malicious activities on the "Protected System", by analyzing the logs on regular basis. The records of unauthorized access, unusual and malicious activity, if any, shall be documented.

- **No. 20(3)/2022-CERT-In, Directions under sub-section (6) of section 70B of the Information Technology Act, 2000** relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet.
- **Central Electricity Authority (Cyber Security in Power Sector) Regulations, 2024.**
- **Minutes of Meeting held under the chairmanship of Secretary (Power) on 'Review of Cyber Security in Power Sector' held on 09.05.2025 and various subsequent advisories.**

Further, successful deployment of Security Information and Event Management (**SIEM**), Security Orchestration Automation & Response (**SOAR**) and End User Behavioural Analysis (**UEBA**) solutions shall also help TPCODL to benchmark itself with other utilities like TPSODL, TPDDL and Tata Power Mumbai respectively.

This initiative is strategically aligned with the corporate objective of enhancing the organization's cyber resilience, protecting critical digital assets, and ensuring compliance with evolving regulatory and operational standards. The proposed investment is intended to Address existing and emerging vulnerabilities across the IT and OT landscape. Strengthen threat detection, prevention, and response capabilities through advanced analytics and automation. Safeguard the critical infrastructure from the cyber threats. Supporting the business continuity and operational reliability by minimizing cybersecurity risks and potential service disruptions. Align with the cybersecurity frameworks and mandates, including **CERT-IN** guidelines, other sectoral regulations and compliances.

By undertaking this investment, the organization aims to build a **robust, proactive, and compliant cybersecurity framework** that underpins the reliability, safety, and trustworthiness of its digital operations.

### **3. Broad Technical Specifications for Proposed Investment**

The proposed investment involves the deployment of advanced cybersecurity technologies aimed at strengthening and modernizing the overall security architecture of Discom. It encompasses network strengthening and expansion augmentation projects, collectively forming a comprehensive defense-in-depth strategy to enhance security, reliability, and resilience across all layers of the IT ecosystem. The initiative will focus on integrating modern security controls, enhancing network visibility, and establishing proactive threat detection and response mechanisms to safeguard critical digital assets, ensure regulatory compliance, and support secure, continuous business operations.

### **4. Capital Structure**

The proposed investment for strengthening the cybersecurity infrastructure is estimated at Rs. 6.24 Crore which will support the procurement and implementation of aforesaid advanced cybersecurity solutions.

## 5. Capitalization Schedule

The above proposed investment for strengthening the Discoms' cybersecurity infrastructure is planned to be capitalized in a phased manner over the implementation period. The capitalization schedule ensures proper allocation of costs to assets, compliance with accounting standards, and transparent tracking of the CAPEX utilization.

The total budget required for this initiative is as mentioned below. This investment covers the costs of technology deployment, infrastructure setup, licensing, and ongoing operational support for the centralized SoC facility.

## 6. Financing Plan

### 6.1. CAPEX Plan

Plan for TPCODL

| All Figures in INR                             |                                     |                               |                                |                   |
|------------------------------------------------|-------------------------------------|-------------------------------|--------------------------------|-------------------|
| On-prem Hardware with 5 Years Warranty Support | SIEM/SOAR/UEBA Licenses for 5 Years | SIEM/SOAR/UEBA Implementation | Integration with existing SIEM | Total CAPEX       |
| 50,00,000                                      | 55,210,525.49                       | 2,229,166                     | -                              | <b>62,439,691</b> |

**Note:** Cost is based on Budgetary Proposal available.

## 7. Physical Target/ Activity

| Sl. No. | Action/Plan                                                      | Duration          |
|---------|------------------------------------------------------------------|-------------------|
| 1       | Bidding and Vendor Selection (From Approval Date)                | 1.5 Months        |
| 2       | Completion of Technical & Functional Design                      | 1.0 Month         |
| 3       | Implementation of solution including unit / module level testing | 3.0 months        |
| 4       | Integration testing                                              | 1.0 Month         |
| 5       | UAT and sign-off                                                 | 0.5 Month         |
| 6       | Fine Tuning & Go-Live                                            | 1.0 Month         |
|         | <b>Total</b>                                                     | <b>8.0 Months</b> |

## 8. Cost Benefit Analysis

The proposed investment is strategically justified by the substantial financial, operational, and compliance-related benefits that will accrue through risk reduction, regulatory adherence, and operational efficiency.

## 8.1. Tangible (Quantifiable) Benefits

| Benefit Area                                                 | Description                                                                                                                                         | Estimated Annual Value (₹) |
|--------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| <b>Avoided Financial Losses due to Cyber Incidents</b>       | Prevention of potential ransomware, phishing, or data breach attacks that could disrupt power supply, billing systems, or customer data operations. | ₹4 Cr                      |
| <b>Reduced Downtime Costs</b>                                | Enhanced system availability and faster recovery through a unified SOC deployment.                                                                  | ₹2-3 Cr                    |
| <b>Reduced Regulatory Penalties</b>                          | Compliance with CEA, CERT-In, and NCIIIP guidelines minimizes risk of fines and penalties.                                                          | ₹1-2 Cr                    |
| <b>Optimized Operational Efficiency</b>                      | Centralized 24x7 monitoring reduces manpower and manual oversight efforts.                                                                          | ₹1-2 Cr                    |
| <b>Savings on Incident Recovery &amp; Insurance Premiums</b> | Lower post-incident remediation and reduced cyber insurance costs.                                                                                  | ₹1 Cr                      |

**Total Estimated Annual Benefit:** ~₹9–12 Crore which may escalate every year.

## 8.2. Intangible (Non-Quantifiable) Benefits

- Strengthened **cyber resilience** and business continuity for critical infrastructure.
- Enhanced **regulatory and audit readiness**
- Increased **stakeholder confidence** (government, consumers, and partners).
- Improved **visibility and proactive response** through Unified Security Operations Center (SoC).
- Alignment with **ISO 27001:2022**.

## 8.3. Summary of Financial Justification

| Paramotor                                           | Value                              |
|-----------------------------------------------------|------------------------------------|
| <b>Total Project Cost (CAPEX + OPEX) Over 5 Yrs</b> | ₹10.24 Crore                       |
| <b>Estimated Annual Benefit</b>                     | ₹9–12 Crore                        |
| <b>Payback Period (Ref: Table-PayBack)</b>          | ~1 Year                            |
| <b>Compliance &amp; Strategic Alignment</b>         | CEA, CERT-In, ISO 27001:2022, TBEM |

### Table-PayBack

| Parameters                   | Year-1 | Year-2 | Year-3 | Year-4 | Year-5 |
|------------------------------|--------|--------|--------|--------|--------|
| Capex Cost in Rs. Cr (A)     | 6.24   | 0      | 0      | 0      | 0      |
| Opex Cost in Rs. Cr (B)      | 0.8    | 0.8    | 0.8    | 0.8    | 0.8    |
| Total Cost in Rs. Cr (C=A+B) | 7.04   | 0.8    | 0.8    | 0.8    | 0.8    |
| Cumulative Cost in Rs. Cr    | 7.04   | 7.84   | 8.64   | 9.44   | 10.24  |

|                                   |        |   |   |   |   |
|-----------------------------------|--------|---|---|---|---|
| Probable Annual Savings in Rs. Cr | 9      | 9 | 9 | 9 | 9 |
| Pay-Back Period                   | Year-1 |   |   |   |   |

The proposed investment is **financially viable and strategically essential**. The implementation of advanced cybersecurity solutions (SIEM, SOAR and UEBA) will significantly mitigate cyber risk exposure, ensure regulatory compliance, and deliver both **quantitative savings** and **long-term operational resilience**.

## 9. Approval from Board of Directors (BOD)

Attached herewith as Annexure-I



**Certified True Copy of the resolution passed at the  
Board Meeting held on 22<sup>nd</sup> April 2026**

"RESOLVED that an additional capex amounting to ₹ 6.24 crore towards Cyber-Security activities for FY27, be and is hereby approved, subject to the approval of Odisha Electricity Regulatory Commission (OERC).

FURTHER RESOLVED that the Chief Executive Officer and the Chief Financial Officer of the Company be and are hereby severally authorized to do all such acts, deeds, matters, and things as may be necessary or expedient to give effect to this resolution."

Certified True Copy  
For TP Central Odisha Distribution Limited

*Suchitra Dash*

(Suchitra Dash)  
Company Secretary  
ACS No. 24156  
Address: Power House Square, Unit-8,  
Bhubaneswar, Odisha-751012

TP CENTRAL ODISHA DISTRIBUTION LIMITED

(A Joint Venture of Tata Power and Government of Odisha)

Registered Office/Corporate Office: Power House Square, Unit-8, Bhubaneswar, 751012, Tel: 0674-2541575 Web:  
www.tpcentralodisha.com, E-mail: tpcodl@tpcentralodisha.com, CIN: U40109OR2020 PLC032901